UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Seguridad en el Internet

Iván Guajardo Arias
Rol 201730009-4

Fernando Salgado Cortés
Rol 201730027-2

Christopher Silva Zavala
Rol 201730005-1

Redes de computadores I – ELO322

1. Resumen

Existen múltiples métodos para vulnerar a la Internet, es por esto que es de suma utilidad el tener al menos un conocimiento básico de de qué son, cómo actúan y así, poder defenderse ante éstos. Como por ejemplo: evitar que nos roben información bancaria.

2. Introducción

Dada la importancia de las redes de computadores en el diario vivir, éstas suelen ser objetivo de la gente maliciosa, llegando incluso a ser ésta considerada como un delito. A continuación, se hablará brevemente con respecto a las vulnerabilidades de la red.

3. Vulnerabilidades de la red

3.1 Ataques de las redes

A lo largo de los años el internet se ha vuelto algo indispensable para el diario vivir. Esto es apreciable en ejemplos tan simples como lo podrían ser el buscar recetas o algo más rebuscado, como podría ser el controlar remotamente los computadores de una empresa. Como es de esperarse, estando una situación que involucra tanta gente como lo es ésta, es muy propenso que alguien intente corromper el intercambio de información que ocurre en la red.

¿De qué forma ocurre?

Esto puede ocurrir de muchas formas, pero por el lado que a nosotros nos compete, sería abordando el malware.

3.2 Malware

El malware (abreviación de “malicious software” o “software malicioso” en español), como indica su nombre, es software con intenciones perjuiciosas hacia la víctima. El funcionamiento del malware puede apuntar a dañar al equipo afectado, sacar información (cuentas, contraseñas, imágenes),

borrar archivos, etc. ¿Cuál es el sentido de hablar sobre esto para el ámbito que trabajamos? Veremos que hay distintos tipos de software dentro de la red, siendo éste el medio de propagación.

Es importante abordar algunos tipos de malware para poder entender mejor el concepto, así que acá se presentan algunos de los más importantes (existen muchos):

3.2.1 Virus

El virus de computadora, es uno de los malwares más comunes dentro de los tiempos actuales. Es muy simple, consiste principalmente en tan solo dañar archivos, molestar al usuario, entorpecer el funcionamiento del equipo básicamente.

3.2.2 Gusanos

Son programas dañinos que, una vez que hayan infectado el ordenador, realizan copias de sí mismo con el objeto de reproducirse lo mas pronto por medio de red, correo electrónico, dispositivos de almacenamiento, programas P2P, mensajería instantánea, etc.

3.2.3 Troyano

Es un malware diseñado para controlar de forma remota un ordenador, tiene como objetivo infiltrarse, dañar una computadora o el sistema de información sin el consentimiento de su propietario.

Se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado

3.3 Botnet

Un botnet es un malaware que convierte al equipo infectado en un bot[1]. La víctima pasa entonces a ser parte de una botnet (distinguir del malware), que es una red de computadores infectados y dispuestos ante el hacker en cuestión para el propósito que tenga, como sacar información,
Los principales usos dados a estas redes son el spam (ver sección de medios de propagación), robo de información, minería de datos y la realización de ataques distribuidos de negación de servicios.

3.4 Ataque distribuido de negación de servicios

Un ataque DoS tiene como objetivo el denegar a los usuarios los servicios de un servidor. Se lleva a cabo por medio de múltiples solicitudes simultáneas que intentan inundar la memoria del servidor, ralentizando a éste e incluso "bajándolo" por algún tiempo que puede variar. Todo esto genera variedad de problemas para el dueño de host y para los usuarios, pues puede implicar una pérdida de dinero o de tiempo importante.
Hay variedad de ataques DoS, basándose en distintos recursos que se han desarrollado a lo largo de los años. Por lo mismo, se ha necesitado renovar constantemente los protocolos, para que estos no se presten a malos fines; como es el caso de la fragmentación, pues esta, permitía consumir más recursos del host mientras intentaba recopilar fragmentos de paquetes falsos.

3.5 Medios de Propagación

3.5.1 Spam

Los términos correo basura o mensaje basura hacen referencia a los mensajes no solicitados, no deseados y/o con remitente anonimo, generalmente son enviados en cantidades masivas que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

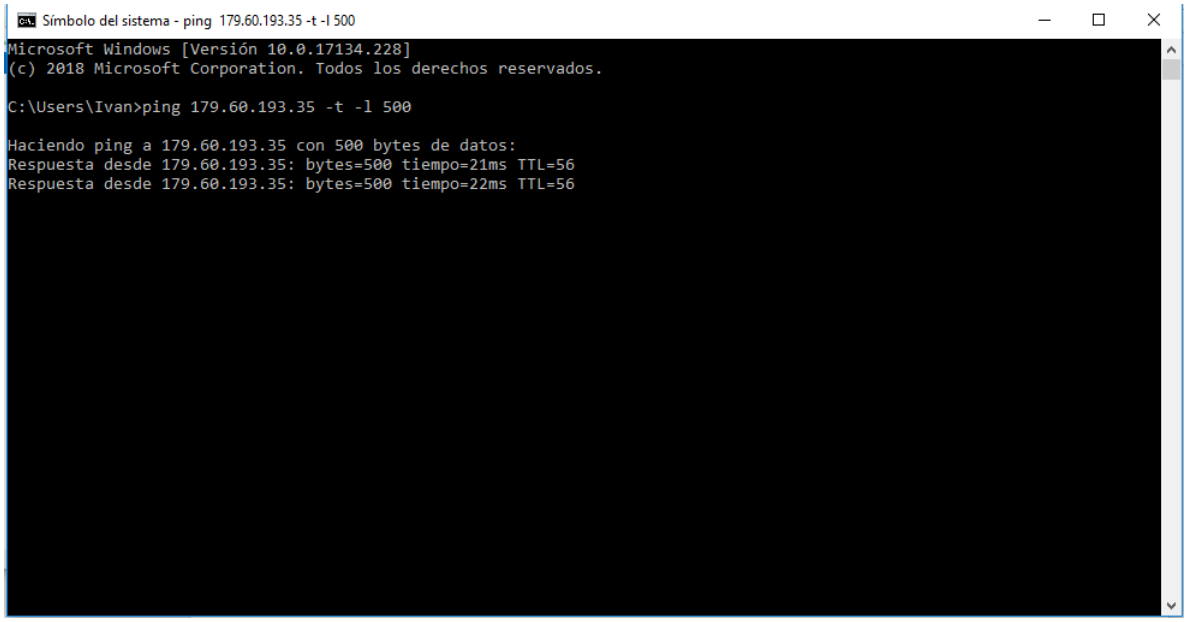
3.5.2 Phishing

“Phishing” como el lector puede imaginarse, surge de "fishing", o "pesca". Por medio de información fraudulenta, el hacker intenta obtener información confidencial del usuario, con la intención de utilizarla después. Es entonces por métodos como correos falsos o suplantación de identidad, que éste puede robar contraseñas de banco (por ejemplo) y así, utilizarla para el fin que se proponga.

3.5.3 Polimorfismo

Es aquel código que se sirve de un motor polimórfico(motor de cambio) para mutarse a sí mismo mientras mantiene su algoritmo original intacto, es decir, cambiar el formato pero mantener la escencia del programa.

4. Resultados



5. Defensas contra ataques

Para defenderse de ataques realizados desde internet hasta, ataques hechos por virus; Es importante tener un buen antivirus instalado, tener actualizado y el Firewall activo, no hacer clic en enlaces que resulten sospechosos, desconfiar de los correos de remitentes desconocidos y por ende, no estar desinformado.

6. Conclusiones

Es increíble cómo la gente se preocupa de estropear lo que a ellos mismos les resulta un beneficio. Internet lleva "poco tiempo" funcionando, y desde sus inicios, ha tenido enemigos que se preocupan de malear el sistema.

Como hemos visto, actualmente existen numerosos métodos para atacar a las redes; no obstante, esto es tan solo un esbozo de lo que realmente se puede hacer, incluso sin considerar que a la web le queda una larga vida y una evolución próspera junto a nosotros, lo que implica a su vez que el malware también tendrá que adaptarse, dejando obsoleto el que actualmente vemos como algo atroz.

7. Referencias

-avast.com

-guru99.com

-latam.karpesky.com

-karpesky.es

-chuiso.com

-Libro guía del ramo